High Ground over the Homeland: Issues in the Use of Space Assets for Homeland Security

by

Lt Col (sel) S. Didi Kuo, PhD, USAF

How the U.S. Develops the potential of space for civil, commercial, defense and intelligence purposes will affect the nation's security for decades to come.

—Commission to Assess United States National Security:
Space Management and Organization
January 2001

THE ATTACK ON 11 September 2001 (9/11) has forever altered how Americans view their security at home. Homeland security is now a top priority for our country in the new war on terrorism. That attack has also transformed our government's approach to defending the homeland. Space assets are being used in the overseas battle against terrorism in intelligence gathering and support of military operations. Space-based surveillance also provides early warning for national missile defense.[1] However, there are several challenges to overcome before we can fully integrate space assets into the homeland-security framework for operations within our US borders.

Lt Col (sel) S. Didi Kuo (USAFA; PhD, Rochester Institute of Technology) is the deputy director of the Space Based Laser Division of AF Space Command's Space and Missile Center. His experience includes assignments at the National Reconnaissance Office, Maui Space Surveillance Site, and the AF Research Laboratory. In addition, he served as a government advisor to the AF Science Advisory Board. Colonel Kuo's publications include "Synthetic Image Generation for Hyperspectral Applications," which appeared in the April 2000 edition of *Optical Engineering;* and "Real Time Orbit Determination of Orbital Space Debris," published in the *Massachusetts Institute of Technology Lincoln Laboratory Space Surveillance Workshop Proceedings* of March 1993. He is a graduate of Squadron Officer School, Air Command and Staff College, and the Defense Systems Management College's Advanced Program Managers Course.

Space Capabilities for Homeland Security

Space already plays an important role in the area of navigation and communication, and it provides the information infrastructure necessary for homeland security. Use of communication satellites, especially commercial ones, provides the backbone for many of the current homeland-security communication needs. The reliance on these satellites becomes even more critical in a crisis where terrestrial communications (both landlines and cellular) are unavailable.[2] Satellite communications provided a message of "assurance and resolve" at a time when the public-accessible communications infrastructure was in disarray.[3]

The Global Positioning System's (GPS) constellation of over 24 satellites has revolutionized the navigational field.[4] After 9/11, GPS attracted attention for its potential uses in homeland security as well as a terrorist target.[5] The integration of GPS into search and rescue and other emergency services is already widespread. After 9/11 major city leaders envisioned how GPS could be used to track certain vehicles and their contents.[6] Surveillance of vehicles belonging to suspected terrorists could also be done through GPS tagging devices. During a crisis response, all emergency vehicles, and even individual personnel, could be tracked by GPS by the Federal Bureau of Investigation's (FBI) Joint Operations Center. The discontinuation of "selective availability" increased the positional accuracy for civil users. The military, however, still receives greater positional accuracy because their encrypted receiv-

Reprinted from *Air and Space Power Journal*, Vol. XVII, No. 1, Spring 2003, pp. 47–56. Published 2003 by Air University Press. Available on the Internet at http://www.airpower.maxwell.af.mil/airchronicles/apj/apj03/spr03/kuo.html

ers can better compensate for ionospheric error.[7] A study should be conducted to determine if homeland-security applications would benefit from that greater positional accuracy.

Weather information from satellites aids in preparedness and consequence management efforts. Real-time environmental data supports vulnerability and risk analyses while forecasts support the decisions that will guide preparation, protection, response, and recovery operations.[8] After the 9/11 attack, the National Weather Service provided this information using special forecasts to assist decision makers in their recovery efforts.[9] Forecasting and real-time data were also provided in support of Operation Noble Eagle.[10]

Overhead signals intelligence (SIGINT) collection can aid in the detection and prevention of terrorist attacks. SIGINT's greatest potential lies in communications intelligence (COMINT)—the interception, monitoring, and location of communications systems and their voice content.[11] In light of the extensive planning done for 9/11, it is clear that domestic surveillance was not as aggressive as it should have been.[12] COMINT derived from space sensors is an additional tool to be added to the terrestrial COMINT systems for the collection of needed intelligence on terrorists in the United States.[13]

Remote sensing is perhaps one of the biggest contributions space can make to homeland security. It has long been used for intelligence and environmental purposes and has seen tremendous growth in the last decade through commercial and civil systems. National systems provide overhead imagery intelligence (IMINT) in the form of high-resolution images. Commercial and civil satellites can collect additional lower-resolution imagery.[14]

Remote sensing from space will play a role in homeland-security preparedness that very much resembles its counterpart mission in the military-intelligence preparation of the battlefield (IPB).[15] The National Spatial Data Infrastructure program is attempting to provide geographical information systems (GIS) for major cities to assist with preparedness for terrorist attacks.[16] Imagery with GIS data could be used to map political and governmental facilities, lines of communication (LOC), choke points such as bridges and tunnels, food and water distribution points, and nuclear facilities. This information can be used both during threat assessments of potential terrorist targets and to aid first responders immediately after an attack.

In the area of response and recovery, remote sensing can be used in assessing thermal activity, the damage to infrastructure, the accessibility to damaged areas, and displacement of debris.[17] Satellite imagery was used a day after the 9/11 attack to aid in the recovery efforts.

> Satellites may provide the quickest means to gain situational awareness, especially when wide-area coverage is needed. More importantly, they can provide a single integrated picture of an incident area. Remote sensing data can be used to aid responders in formulating a proper response, such as evacuation routes for a weapon-of-mass-destruction attack.[18]

Homeland-Security Customers

Table 1 shows the actual and potential uses of space-asset capabilities by homeland-security organizations. Some agencies have already integrated space components into their operations. Many agencies consider GPS and satellite communications to be inherently part of their information infrastructure. Other systems, most notably intelligence, surveillance, and reconnaissance (ISR) satellites, are still relatively unused. The next section discusses reasons for this underutilization.

Issues on the Use of Space for Homeland Security

Space communication, navigation and weather systems are designed for use within the United States and are well integrated into the federal, civil, and commercial sectors. As a result, there are no major limitations on their use in the homeland-security mission. However, with the exception of commercial imagery, the focus of ISR systems has been on overseas areas. The national ISR space architecture, ranging from satellite orbits to the infrastructure on the ground, is geared towards supporting military operations and intelligence gathering on foreign soil. Prior to 9/11, the defense and intelligence communities did not perceive a need for the use of ISR space assets in homeland security. Now, however, several organizations are examining the contributions ISR space can make to this new mission.[19]

The Space Community: Black or White?

Multiple organizations build and operate satellites for the US government because of the many national security space missions performed. The national security space community is still largely divided between unclassified Department of Defense (DOD) systems (the white world) and clas-

Table 1
The Use of Space Assets by Homeland-Security Agencies

Homeland-Security Agency	*Major Areas of Space Support*
US Northern Command	ISR, Communication, Navigation, Weather, and Remote Sensing
Federal Bureau of Investigation	ISR, Communication, and Navigation
Federal Emergency Management Agency	Remote Sensing, Mapping, Communication, Weather, and Navigation
National Infrastructure Protection Center	Remote Sensing, Mapping, and Navigation
Office of Domestic Preparedness	Remote Sensing, Mapping, and Navigation
US Border Patrol	ISR, Remote Sensing, and Navigation
US Coast Guard	Navigation, Communication, and Weather
Environmental Protection Agency	Remote Sensing
Department of Energy	Remote Sensing
US Customs	Navigation
State and Local Law Enforcement Agencies	ISR and Navigation
State and Local Emergency Services	Communications, Navigation, Weather, and Remote Sensing
National Guard	Communication, Navigation, Weather, and Remote Sensing

sified intelligence systems (the black world). On the DOD side, Strategic Command is responsible for coordinating all military and civilian space assets while Air Force Space Command acquires and operates the majority of military satellites. The National Reconnaissance Office (NRO) is responsible for the acquisition and operation of the nation's intelligence satellites, often known as national technical means (NTM).

Recent Space Commission recommendations generated several organizational changes in the national security space community.[20] The undersecretary of the Air Force (USecAF) became responsible for DOD space as well as serving as the director of the NRO. While implementing the Space Commission recommendations should improve interagency coordination, some organizational issues will remain.[21] The NRO commission stated that the NRO is caught between the competing requirements of its DOD and intelligence community customers.[22] An independent Commission on the National Imagery and Mapping Agency (NIMA) called this the "national versus tactical" problem and found it to be a highly polarizing issue.[23] Until the recent implementation of the Space Commission recommendations, only the president had the authority to provide the leadership, direction, and oversight for a coherent national security space policy.[24] Even with the USecAF's new responsibilities and authority, it remains to be seen if these old barriers can be dismantled.

There are three important issues to consider when defining homeland-security roles and missions for space: competition between space missions, customer requirements, and funding. The first issue is how much the homeland-security mission will compete with other space missions for the same resources. Homeland-security requirements will not significantly affect GPS because of its inherent design for civil applications. US Northern Command (NORTHCOM) will dominate DOD's requirements, and the ability of military communication satellites to support NORTHCOM and other federal agencies will be stressed if there is a major theater war (MTW) and a large-scale terrorist attack in the United States. Under those conditions, there may not be enough secure bandwidth to support NORTHCOM, and additional bandwidth would have to come through commercial communication satellites.

National systems may experience a similar problem during an MTW. These systems not only have to support military operations overseas, but also maintain regular intelligence collections of other nations. The NRO Commission pointed out that customer demands, both strategic and tactical, already exceed the NRO's capabilities.[25] Supporting the homeland-security mission will put an additional burden on the NTM systems. Again, commercial satellites may be able to supplement the collection needs over the United States, especially due to the lack of restrictions on their operations.

The second issue is identifying homeland-security customers and determining their space capability requirements. The organizational landscape for homeland security is vast and often confusing. DOD and other federal agencies are involved at the national level, while state and local organizations play a critical role as first responders. A proper provider-customer relationship between the space and homeland-security organizations is currently lacking and must be developed. Many of these homeland-security-organization customers are not yet aware of the capabilities that space assets offer. For that reason, they have not yet determined their requirements, which further complicates identification of space resources needed for the homeland-security mission.

The third issue is funding. If space assets are to play a role in homeland security, they must be properly funded. This is especially critical for dual-hatted organizations like the NRO, NIMA, and National Security Agency (NSA) that must not only be concerned about the amount of funding but also the funding's source and the legal constraints on its use. Using DOD money on homeland security may violate the Posse Comitatus Act, while the intelligence community dollars are reserved for foreign intelligence collection. In the long-term, the homeland-security mission may even require new capabilities on satellites (i.e., enhanced GPS civil capabilities or new NTM sensors). The new Department of Homeland Security may eventually become the appropriate funding source for the amount of funding that includes proper legal authorization on its use. Until then, programming funds for this capability may be difficult.

The Homeland-Security Landscape

The war on terrorism will truly be an interagency process involving some 40 federal agencies. They will be joined by a host of state and local offices that will be involved in some form of homeland-security activities.[26]

The Department of Homeland Security is responsible for preventing, to the degree possible, terrorist attacks in the United States and aiding in the recovery from such attacks.[27] Three of the assigned functions for this new office may involve advocating the need for space support. The first is to ensure that there are sufficient technological capabilities and resources to collect intelligence and data on terrorist activities within the United States. The second function is to make certain that proper resources are allocated to improve and sustain national preparedness against terrorist threats. The third function is to coordinate the response and recovery efforts to a terrorist attack. Space capabilities can help the Department of Homeland Security carry out these functions.

Currently the DOD role in homeland security is limited. America's long-standing fear of military involvement in domestic affairs has resulted in a myriad of statutes and directives that govern the use of the armed forces within the United States.[28] Key tasks are air and missile defense as well as assisting civilian authorities in responding to natural disasters and terrorist attacks.[29] The National Guard is exempt from many of the restrictions.[30] Until federalized, they belong to their respective states and thus may provide domestic support.[31] Like other homeland-security organizations, the close integration of National Guard units with space assets is limited.

Both *Joint Vision 2020* and the *2001 Quadrennial Defense Review* discuss the importance of homeland security.[32] The creation of NORTHCOM will help focus the DOD's homeland-security mission.[33] NORTHCOM has both North American Aerospace Defense Command's (NORAD) mission of air and space defense as well as US Joint Forces Command's mission of providing military assistance to civil authorities.[34] The need to integrate space operations within the United States, especially ISR systems, means NORTHCOM has unique space issues not encountered with the other geographical commands.

Past experience demonstrates that nonfederal local authorities are normally the first to respond to emergencies and threats.[35] Several studies and reports recommended strengthening the state and local agencies responsible for homeland security.[36] There is a lack of understanding at the state and local levels of what space can do. This is especially true of national systems because of the necessary security clearances. Unless there is an education process among these organizations, new applications of space to homeland security will be limited.

The number of organizations involved in homeland security may be an impediment to the effective use of space for homeland security. Bureaucratic infighting and the lack of clear lines of responsibility make the integration of space into various homeland-security missions difficult. Not only are civil and military agencies involved at

the national level, but state and local agencies will also play a crucial role. To compound this problem, the space community itself is made of multiple organizations that are currently in a state of transition. There is no place for the Department of Homeland Security to go for "one-stop shopping" on space issues. To get all of these moving parts from both communities to work together will be a monumental challenge. While it is out of the scope of this article to solve these homeland-security organizational problems, a solution must be found if space is to be effectively used.

Legal and Policy Limitations: Blindfolding the Eye in the Sky

Obstacles to using ISR satellites for homeland security include the legal and policy issues surrounding the intelligence collection on US persons. While surveillance systems such as the Defense Support Program satellites do not have an issue because of their low resolution, NRO's IMINT and SIGINT satellites have the capability to aid homeland security in this area.[37] In addition, possible new surveillance methods such as GPS tagging will also face legal issues. There has always been a delicate balance between the need for national security and the protection of individual privacy rights under the US Constitution.[38]

Domestic intelligence collection from space is subject to a complex legal and policy landscape with multiple directives that are often open to interpretation. Table 2 illustrates some of these laws and policies.

Executive Order (EO) 12333 establishes the overall framework for all intelligence gathering within the United States. It is the primary guidance for IMINT collections on US soil and provides additional instruction to the Foreign Intelligence Surveillance Act (FISA) for domestic SIGINT collections. Even though NRO satellites collect both SIGINT and IMINT, NSA and NIMA have additional and different guidance for this process.[39]

FISA regulates the collection of SIGINT on US persons.[40] This classified document requires a special court order to collect SIGINT within the United States. The Bremer Commission found that under ordinary circumstances, the FISA process can be slow and burdensome.[41] The reviewing agency often used stricter interpretations requiring more information than mandated by FISA.[42] Additional guidance for SIGINT comes from the United States Signals Intelligence Directive 18.[43] This NSA directive ensures that these types of collections are conducted in a manner that safeguards the constitutional rights of US persons.

Because the NRO, NSA, and NIMA are also affiliated with the DOD, Title 10 issues such as the Posse Comitatus Act may apply to them. A review of the literature quickly shows there is no universal agreement on what the Posse Comitatus Act allows and forbids the military to do in homeland security.[44] While most DOD space operations within the United States are considered passive and thus permitted under this act, intelligence satellites play a more active role. As a result, the NSA and NIMA may be prohibited from distributing NTM products under the Posse Comitatus Act because they are DOD support agencies.

As table 2 illustrates, there are many legal and policy constraints on NTM activities and what it collects in the United States. Much of this direction overlaps itself, and almost all of it is subject to interpretation. One example is that both DOD and the intelligence community regulations apply to NIMA. Must NIMA use the most restrictive guidance to limit its operations, or can it use the most advantageous policy to provide imagery? Unless such issues are resolved in advance, timely distribution of NTM products is unlikely in a critical situation. Now is the appropriate time to revise these regulations in order to provide greater latitude for intelligence collection from space within the United States.

The TPED Issue Hits Home

Tasking, processing, exploitation, and dissemination (TPED) of national space products is currently a major hindrance to fully utilizing these assets. The problem of having sufficient resources to get the product to the military user in the field has been widely identified.[45] The same challenge will be faced when getting the product out to homeland-security agencies, especially in a timely manner. NIMA is responsible for national IMINT space products, while NSA is responsible for SIGINT space products. Both of these organizations have come under scrutiny for their performance of that role.[46] The addition of the homeland-security mission will only increase the strain on their already overburdened TPED resources.

On the tasking side, the homeland-security agencies need to understand what they can task and how to frame the request for collection so

Table 2
Major Regulations Affecting the Use of Space for Homeland Security

Regulation	*Type*
Executive Order 12333, United States Intelligence Activities	Executive Directive
Executive Order 12958, Classified National Security Information	Executive Directive
Presidential Decision Directive 35, Intelligence Requirements	Executive Directive
Presidential Decision Directive 39, US Policy on Counterterrorism	Executive Directive
Presidential Decision Directive 49, National Space Policy	Executive Directive
Foreign Intelligence Surveillance Act (50 USC)	Statute
USA PATRIOT Act	Statute
Posse Comitatus (10 USC 1385)	Statute
National Security Act of 1947 (50 USC)	Statute
Classified Information Protection Act (18 USC)	Statute
Freedom of Information Act (5 USC 552)	Statute
DOD Directive 5525.5, *DOD Cooperation with Civilian Law Enforcement Official*	Department Policy
DOD Directive 3025.1, *Military Support to Civil Authorities*	Department Policy
DOD Directive 5240.-R, *DOD Activities That May Affect US Persons*	Department Policy
CIA Headquarters Regulation 7-1, *Law and Policy Governing the Conduct of Intelligence Activities*	Department Policy
US Signals Intelligence Directive 18	Department Policy
United States v. Kyllo (2001)	Judicial Ruling
United States v. Katz (1966)	Judicial Ruling
United States v. Dow (1983)	Judicial Ruling

that it can be done legally. While NIMA is in the process of streamlining the approval process for domestic imaging, requests still must come through other federal agencies.[47] During time-critical events, this bureaucratic delay can result in missed opportunities by satellites with limited observation windows. For processing and exploitation of space products, the homeland-security agencies have neither the same expertise nor tools as the space and TPED organizations. An inadequate distribution infrastructure also hampers the dissemination of NTM products. One option is to provide special equipment to homeland-security agencies that can receive and exploit NTM imagery, similar to what is being done for military units.[48] Classification of the products is another issue. A way is needed to rapidly declassify the information so that local responders can use it in a timely manner. For IMINT, the image can be degraded or used as a source for a derived product. For SIGINT, information needs to be disseminated without attribution to the NSA.

Because state and local agencies play a vital role in homeland security, the national TPED capabilities must reach down to the local levels.[49] Currently the availability of NTM products to these agencies is almost nonexistent. The increasing availability of commercial imagery may improve this situation. Because state and local authorities are typically the first responders, it is imperative to extend the TPED process down to this level.

Commercial Imagery: The New Satellite on the Block

A discussion on the use of space for homeland security would not be complete without mentioning the growing role of commercial space imagery. A commercial satellite owned by Space Imaging took some of the most widely recognized pictures of the 9/11 attack.[50] The New York governor's office contacted Space Imaging directly to request information on the use of satellite imagery for disaster assessment and emergency management.[51] It was an unusual situation where a state went directly to a private company rather than a federal agency for help on using space assets. As second-generation satellites

with improved resolution are launched the importance of commercial imagery for homeland security will become even more pronounced.

The two main advantages of commercial imagery are the lack of legal restrictions on their use over the United States and the unclassified nature of their product. Because they are privately owned, commercial systems do not face the same restrictions as national systems. Their unclassified products can easily be distributed to anyone, provided the proper licenses are bought. This is important because many homeland-security agencies, especially at the state and local levels, do not have the necessary security clearances for national imagery. Also, the dissemination of these products can be done through the Internet, thus providing quick and easy access. Because of these advantages, commercial imagery, as it becomes more available, will be a major source of data from space for homeland security.

The High Ground for Homeland Security

Space assets can play a significant role in enhancing homeland security. These systems provide communication and navigation support that is vital to homeland-security functions. Satellites also provide unique information from their vantage point in space. Whether it is providing intelligence against a terrorist threat or preparing and responding to a WMD attack, space provides unfettered access to quickly collect information over wide areas at any location in the United States. Despite these capabilities, significant legal, policy, organizational, and procedural limitations exist. These limitations must be examined and addressed if space is to be fully utilized for homeland security.

The same situation for the use of space in homeland security today existed with the military in Desert Storm. Many space assets were an unknown quantity when planning for operations at that time. Only after 10 years of effort is space now an integral part of military operations, as demonstrated in Operation Enduring Freedom. The challenge now is using space for this new national security threat. The Department of Defense and the Department of Homeland Security must now work together to bring the high ground home to America.

Notes

1. The Defense Support Program (DSP) satellites, a key part of North America's early warning system, detect missile launches, space launches, and nuclear detonations. The Space-Based Infrared System (SBIRS) is scheduled to replace it.

2. Immediately after the 9/11 attacks, cell phone use was unavailable both in Manhattan and Washington, D.C., due to overwhelming usage.

3. This was the comment made by Richard DalBello, executive director of the Satellite Industry Association, at the 18th National Space Symposium.

4. For an excellent review of how GPS is used worldwide, see National Aeronautics and Space Administration's GPS homepage at http://gpshome.ssc.nasa.gov/. For a tutorial on how GPS works, see Jeff Hurn, *GPS: A Guide to the Next Utility* (Sunnyvale, Calif.: Trimble Navigation, 1989). Additional information can also be found on-line, GPS Joint Program Office Web site available from http://gps.losangeles.af.mil.

5. "Terrorism Attacks Accelerate Interest in GPS Applications," SpaceDaily.com, 1 December 2001, on-line, Internet, 28 February 2002, available from http://www.spacedaily.com/news/gps-01s.html.

6. Although a contract was awarded by an unnamed city to do this, no specific details were given. I have speculated on what some of the applications might be.

7. The Standard Positioning Service provides civil users a minimum of 36-meter accuracy (based on a worst-site positioning-domain accuracy at 95 percent all-in-view horizontal error).

8. Donald Wernly, "NOAA's (National Oceanic and Atmospheric Administration) Capabilities to Support Homeland Security," presentation to the Committee for Operational Processing Centers (COPC) and Shared Processing Operations Steering Committee (SPOSC) Meeting, Camp Springs, Md., 28 November 2001, on-line, Internet, 28 February 2002, available from http:// www.ofcm.gov/copc/copc_meeting-01-2.htm.

9. "NOAA's Role in the Nation's Recovery Efforts and the War on Terrorism," *NOAA Magazine,* 1 November 2001, on-line, Internet, 15 January 2003, available from http://www.noaanews.noaa.gov/magazine/stories/mag2.htm.

10. Col Bob Allen, "Air Force Weather Agency Director's Update," presentation at the COPC/SPOSC Meeting, 28 November 2001, on-line, Internet, 28 February 2002, available from http://www.ofcm.gov/copc/copc_meeting-01-2.htm.

11. SIGINT can be broken into electronic intelligence (ELINT), foreign instrumentation signals intelligence (FISINT), and communications intelligence (COMINT). ELINT and FISINT are used to collect information on radars, weapon systems, and telemetry, and probably would not be of much utility since terrorists are unlikely to use weapons of that sophistication. Definitions of these three types of SIGINT can be found in Air Force Doctrine Document 2-5.2, *Intelligence, Surveillance, and Reconnaissance Operations,* 21 April 1999, 27, on-line, Internet, 28 February 2002, available from https:// www.doctrine.af.mil/ Main.asp.

12. Kurt Campbell and Michele Flournoy, *To Prevail: An American Strategy for the Campaign against Terrorism* (Washington, D.C.: Center for Strategic and International Studies Press, December 2001), 79.

13. This collection is already done overseas, although there have been questions raised on the ability to track terrorists who may limit their electronic conversations.

14. The Department of Energy's Multi-Thermal Imager provides both mid-wave and long-wave infrared imagery. LANDSAT, SPOT, IKONOS, and Quickbird have four to seven

multispectral bands. Canada's RADARSAT provides synthetic aperture radar (SAR) imagery.

15. IPB is defined as the continuous process used to develop a detailed knowledge of the adversary's forces and capabilities.

16. The NSDI falls under the auspices of the Federal Geographic Data Committee chartered by the Office of Management and Budget. For more information, visit their Web site on-line at http://www.fgdc.gov/nsdi/nsdi.html.

17. These were the type of questions asked to the remote sensing community after the 9/11 attacks. Senate Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services, "Assessment of Remote Sensing Data Use by Civilian Federal Agencies," 10 December 2001, 10.

18. A Domestic Emergency Support Team (DEST) would provide on-scene expertise for nuclear, biological, and chemical attack.

19. Some conferences held to address these issues were the Chamber of Commerce Space Enterprise Council's forum on the use of space for homeland security held on 8 November 2001, the NRO's Federal Reconnaissance Conference held on 4 February 2002, and the National Defense Industrial Association's Changing Face of Military Space Conference on 26 February 2002.

20. Hon. Donald Rumsfeld, secretary of defense (SECDEF), memorandum to secretaries of the military departments et al., subject: National Security Space Management and Organization, 18 October 2001.

21. Even a year after the release of the Space Commission, one panel member stated that many of the same problems still exist.

22. Report of the National Commission for the Review of the National Reconnaissance Office: The NRO at the Crossroads (NRO Commission), 1 November 2000, on-line, Internet, 16 January 2003, available from http://www.fas.org/irp/nro/commission/nro.pdf. The NRO Commission called on the SECDEF and director of Central Intelligence (DCI) to work closely together to balance these needs.

23. Independent Commission on the National Imagery and Mapping Agency, *The Information Edge: Imagery Intelligence and Geospatial Information (NIMA Commission),* December 2000, on-line, Internet, 16 January 2003, available from http://www.fas.org/irp/ agency/nima/commission/report.pdf. See section 8.2 and 10.1 where it notes that several capabilities desired by the JCS in the NRO's future imaging architecture were unable to be met because of cost constraints.

24. Commission to Assess United States National Security: Space Management and Organization (Washington, D.C., 11 January 2001), on-line, Internet, 16 January 2003, available from http://www.defenselink.mil/pubs/spaceintro.pdf. See "Executive Summary," 19.

25. NRO Commission, "Executive Summary."

26. Center for Defense Information Terrorism Project, "Organizations for Homeland Security: Issues and Options," 21 December 2001, on-line, Internet, 28 February 2002, available from http://www.cdi.org/terrorism/homelandsecurity.cfm.

27. The Department of Homeland Security, June 2002, on-line, Internet, 10 July 2002, available from http://www.whitehouse.gov/deptofhomeland/book.pdf.

28. John R. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," *ANSER Institute Homeland Defense Journal,* February 2002, on-line, Internet, 28 February 2002, available from www.homelandsecurity.org/journal/articles/displayarticle.asp/ article=30.

29. Dale Eisman, "Command of Homeland Defense Combines Parts of 2 Agencies," *The Virginian-Pilot,* 6 February 2002, A-6.

30. The National Guard and Reserve operate under Title 32, not Title 10, and thus are exempt from the Posse Comitatus Act.

31. Gen Russell C. Davis, "The National Guard: Americans at Their Best," lecture, Air Command and Staff College, Maxwell AFB, Ala., 6 February 2002.

32. *Joint Vision 2020* highlights the need for interagency cooperation when dealing with HLS. In the *QDR,* released weeks after 9/11, HLS was cited as a top priority for the military.

33. Secretary of Defense Donald Rumsfeld, "21st Century Transformation of the U.S. Armed Forces," speech, National Defense University, Washington, D.C., 31 January 2002.

34. Chairman of the Joint Chiefs of Staff, Joint Publication 1, *Joint Warfare of the Armed Forces of the United States,* 14 November 2000.

35. Jeffery Brake, "Terrorism and the Military's Role in Domestic Crisis Management: Background and Issues for Congress," CRC Report for Congress, 19 April 2001.

36. *Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,* pt. 3, Third Annual Gilmore Report (Washington D.C., 15 December 2001), on-line, Internet, 28 February, 2002, available from http://www.rand.org/ nsrd/terrpanel/terror3-screen.pdf., iv.

37. Since the National Security Act of 1947 stated the CIA "shall have no … internal security functions," there have been strict guidelines on NTM collections over the United States.

38. For an excellent discussion of this topic, see Stewart Baker, "Shall Spies Be Cops?" *Foreign Policy,* no. 97 (winter 1994/95): 36.

39. For SIGINT, NSA follows DOD Directive 5240.1-R and US Signals Intelligence Directive 18. For IMINT, NIMA follows DOD Directive 5525.5.

40. A US person is defined as a citizen of the United States or an alien lawfully admitted for permanent residence. In the FY 2000 Intelligence Authorization Act, the FISA standards were reemphasized on SIGINT collections. FY 2000 Intelligence Authorization Act, Legal Standards for the Intelligence Community in Conducting Electronic Surveillance (Washington, D.C.: February, 2000).

41. *Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism,* The Bremer Commission (Washington, D.C.: 7 June 2000), on-line, Internet, 28 February 2002, available from http://www.terrorism.com/documents/ bremercommission/index.shtml, chap. 2.

42. The Department of Justice's Office of Intelligence Policy and Review (OIPR) must first approve FISA orders. In practice the OIPR required additional evidence of wrongdoing or specific knowledge of the group's terrorist intentions in addition to the person's membership. The Bremer Commission recommended that the attorney general order the OIPR not to require information in excess of FISA standards. The Bremer Commission, chap. 2.

43. US Signals Intelligence Directive (USSID) 18 is classified; however, a declassified version can be found on-line.

44. John R. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," *ANSER Institute Homeland Defense Journal,* February 2002, on-line, Internet, 28 February 2002, available from http://www.homelandsecurity.org/journal/articles/displayarticle.asp/ article=30.

45. The NIMA Commission, "Executive Summary."

46. Ibid.; and Bill Gertz, "Spy Data Analysis Criticized as Slow," *Washington Times,* 25 October 2001, 14.

47. Catherine MacRae, "NIMA Eyes Simpler Process to Share Intel with Domestic Authorities," *Inside the Pentagon,* 11 July 2002, on-line, Internet, 11 July 2002, available from ebird.dtic.mil/Jul2002/s20020711nima.htm.

48. Some examples of these exploitation tools that can be deployed to the field include the NIMA In-a-Box for Leveraged Exploitation (NIMBLE), Broadcast-Request Imagery Technology Experiment (BRITE), and Eagle Vision.

49. This was highlighted by the director of NIMA at a recent symposium. "Clapper: NIMA Transforming to Respond to Homeland Defense Role," *Aerospace Daily,* 11 April 2002.

50. Pictures shown in this article are available on the Space Imaging Web site, www.spaceimaging.com.

51. David Leonard, "Private Satellites Primed for National Security Role," *Space News,* 14 September 2001, on-line, Internet, 28 February 2002, available from http://space.com/news/remote_ surveillance_010914-1.html.
